U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON
SCIENCE, SPACE, & TECHNOLOGY

Opening Statement

Chairwoman Kendra Horn (D-OK)
of the Subcommittee on Space and Aeronautics

Space and Aeronautics Subcommittee Hearing:
Cybersecurity at NASA: Ongoing Challenges and Emerging Issues for Increased Telework During COVID-19

Friday, September 18, 2020

Good morning. I'd like to welcome our distinguished panel of witnesses, Members, and those viewing remotely, to today's Space and Aeronautics Subcommittee hearing on "*Cybersecurity at NASA: Ongoing Challenges and Emerging Issues for Increased Telework During COVID-19*".

In early 2020, the world was caught off guard with the rapid and dramatic onset of the coronavirus. NASA, like many Federal agencies, and consistent with Office of Management and Budget guidance, rapidly shifted to telework operations to ensure the health and safety of its more than 17,000 civil servant employees and extensive contractor workforce.

To its credit, NASA prepared for the transition, having held an agency-wide telework exercise in early March to test expanded telework operations. Today, 75 to 80 percent of NASA civil servants continue to work remotely handling proposal reviews, project oversight and inspections, development work, engineering analysis, and other activities.

The shift to increased telework at NASA raises many questions. Front and center is cybersecurity.

- What does the increase and extended use of telework mean for protecting NASA' intellectual property, personally identifiable information, and mission operations?
- How do the cyber challenges related to increased telework affect the agency's overall cybersecurity risk posture?
- And what steps is NASA taking to ensure the effectiveness of its cybersecurity efforts during the pandemic and beyond?

These are some of the questions today's hearing will explore, because what's clear is that NASA is a target.

A recent NASA IG report stated, "Given NASA's mission and the valuable technical and intellectual capital it produces, the information maintained within the Agency's IT infrastructure presents a high-value target for hackers and criminals."

In early 2019, NASA Administrator Jim Bridenstine stated at an agency town hall that "NASA is one of the—it is the most attacked agency in the Federal government when it comes to cybersecurity." Past data breaches and system intrusions at NASA and its facilities have resulted in large amounts of stolen data; installation of malware; copying, modifying, and deleting sensitive files; and accessing NASA servers, including those supporting missions.

The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency—CISA—has issued specific alerts on vulnerabilities related to telework during the pandemic and encourages organizations "to adopt a heightened state of cybersecurity."

In April 2020, the agency's then-chief information officer notified employees of increased hacking attempts on the agency's systems. And in June 2020, media articles reported that malicious actors congratulated NASA and SpaceX on a crewed demonstration flight, and then announced they had allegedly breached and infected a NASA contractor, specifically one that provides information technology and cybersecurity services to the agency. If true, that's a concerning report, and part of the reason we're here today.

Protecting NASA's IT and data during the pandemic demands vigilance. However, NASA's cybersecurity challenges don't begin and end with the COVID crisis. Multiple NASA IG and GAO reports have identified weaknesses and ongoing concerns with NASA's information security; further, they have ranked the issue as a top agency challenge.

Ensuring effective cybersecurity at NASA becomes even more pressing, given rapid advances in IT, supply chain risks, NASA's culture of openness and partnerships, and the overall increase in space activities.

NASA is a national treasure. Its missions continue to inspire both young and old and NASA's cutting-edge space technologies, research, and spaceflight experience are the envy of the world. NASA's accomplishments wouldn't be possible without computers, software, and information systems.

Will NASA or any organization ever be 100 percent risk-free from cyber threats? Probably not. Is there room for improvement? Most definitely, yes.

I hope today's hearing will give us an understanding of the challenges and risks posed by increased telework, and whether or not NASA is organized and resourced to effectively mitigate those risks. Bottom line: we need to ensure that NASA has the tools and takes the necessary actions to ensure the agency's success, safety, and security, during COVID, and beyond.

I look forward to our witnesses' testimony.